UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------x

ZAP CELLULAR, INC., doing business as AMP Cellular,

Plaintiff,

- against -

ARI WEINTRAUB, MORTON WEINTRAUB, ESTI DRESDNER, STEVE WEINSTOCK, and MAZAL TECH MEDIA, INC.,

Defendants.

----------x

**MEMORANDUM & ORDER**
15-CV-6723 (PKC) (VMS)

PAMELA K. CHEN, United States District Judge:

On November 23, 2015, Plaintiff Zap Cellular, Inc., d/b/a Amp Cellular ("Zap"), filed this lawsuit against Defendants Ari Weintraub ("A. Weintraub"), Morton Weintraub ("M. Weintraub"), Esti Dresdner, Steve Weinstock, and Mazal Tech Media, Inc. ("Mazal"). (Complaint ("Compl."), Dkt. 1.) Plaintiff alleges that A. Weintraub, the former Chief Executive Officer ("CEO") of Zap and current CEO of Mazal, violated Sections 1030(a)(2) and 1030(a)(5)(C) of the Computer Fraud and Abuse Act (the "CFAA"), and that all Defendants violated various state laws, by engaging in a scheme where Mazal—Zap's former customer payment processor—continued billing Zap customers after A. Weintraub was terminated as Zap's CEO and the Zap-Mazal payment processing agreement had expired. (*Id.* ¶¶ 49–112.)

At a May 13, 2021 pretrial conference—held after years of discovery and motion practice—Defendants informed the Court of their desire to move for judgment on the pleadings for lack of subject matter jurisdiction. (05/13/2021 Docket Entry.) Defendants' motion is now fully briefed. Defendants argue that (1) the Court lacks subject matter jurisdiction over M. Weintraub, Dresdner, Weinstock, and Mazal because no federal claims are alleged against them;

(2) the CFAA claims against A. Weintraub fail as a matter of law because (a) A. Weintraub had authorization to access Plaintiff's computers and servers and (b) Plaintiff did not suffer a "loss" cognizable under the CFAA; and (3) with Plaintiff's CFAA claims dismissed, this Court should decline to exercise supplemental jurisdiction over Plaintiff's state law claims.

Defendants are incorrect on all counts. First, as all of the parties have correctly assumed throughout this litigation, the Court has supplemental jurisdiction over the claims against M. Weintraub, Dresdner, Weinstock, and Mazal because they stem from the same common nucleus of operative fact as Plaintiff's CFAA claims against A. Weintraub. Second, the Complaint plausibly alleges that A. Weintraub's authorization to access Plaintiff's computers and servers was revoked when he was terminated as CEO and Mazal's contract with Zap expired, and that Plaintiff has suffered a "loss" cognizable under the CFAA. Third, even if the Court were to dismiss Plaintiff's CFAA claims, it would continue to exercise supplemental jurisdiction over Plaintiff's state law claims given the time and effort already invested in this case. Accordingly, Defendants' motion for judgment on the pleadings is denied in its entirety and the parties will file a new joint pretrial order, as explained below.

## BACKGROUND

### I. Factual Background[1]

Plaintiff is "an international telecommunications company" that "provides telecom products and services to consumers." (Compl., Dkt. 1, ¶ 9.) Plaintiff secures its customer payment

[1] Because the standards of review for Rule 12(c) and Rule 12(b)(6) motions are identical, *Lively v. WAFRA Inv. Advisory Grp., Inc.*, 6 F.4th 293, 301 (2d Cir. 2021), the Court "accept[s] as true all factual allegations [from the Complaint] and draw[s] from them all reasonable inferences; but [it is] not required to credit conclusory allegations or legal conclusions couched as factual allegations." *Hamilton v. Westchester Cnty.*, 3 F.4th 86, 90–91 (2d Cir. 2021) (quoting *Dane v. UnitedHealthcare Ins. Co.*, 974 F.3d 183, 188 (2d Cir. 2020)).

information with an Authorize.Net account, and uses a third-party vendor to process payments from customers. (*Id.* ¶¶ 11, 13.) From about May 2013 until August 2013, Zap contracted with Mazal to provide this service, authorizing Mazal to access its customer payment information through Authorize.Net and to charge for services rendered by Zap. (*Id.* ¶¶ 13–15.) Following each billing cycle, Zap sent statements to customers and informed Mazal how much to charge the customers, and Mazal charged customers accordingly. (*Id.* ¶¶ 14–15.) Mazal deposited customer's payments into a Mazal bank account (the "Mazal Account"), which was solely dedicated to Zap transactions and was controlled by an officer of Zap. (*Id.* ¶¶ 16–17.) In addition, A. Weintraub, the CEO of Mazal, was also CEO of Zap, which authorized him to "access . . . accounts, passwords, and other administrative information belonging to [Zap]." (*Id.* ¶¶ 18–20.)

After the August 2013 billing cycle, Zap and Mazal agreed to discontinue their business relationship, and Mazal was no longer authorized to process the credit cards of Zap customers. (*Id.* ¶¶ 25–26.) In September 2013, A. Weintraub's position as Zap CEO was terminated. (*Id.* ¶¶ 20 (stating A. Weintraub's authorization was based solely on his employment), 27, 28.) As a result, A. Weintraub's was no longer authorized to access Zap's computers and servers to obtain customer and billing information. (*Id.* ¶ 56, 66, 67, 68, 73, 78, 84, 90.)

Following his termination, A. Weintraub schemed with Defendants M. Weintraub, Esti Dresdner, and Steve Weinstock to defraud Plaintiff's customers by opening a Mazal merchant bank account, continuing to access Plaintiff's computers and servers—without authorization—to obtain Plaintiff's confidential customer and billing information, bill Plaintiff's customers, and deposit the proceeds into Mazal's merchant bank account. (*Id.* ¶¶ 29–38.) Defendants billed Zap customers the amount owed to Zap for its September 2013 services and continued billing Zap

customers until at least January 2014, depositing the proceeds in Mazal's merchant bank account. (*Id.* ¶¶ 33–41.)

In January 2014, Plaintiff sent a communication to its customers asking them to contact their credit card companies to report the charges as fraudulent, but Defendant A. Weintraub then, without authorization, "accessed an external [] email server [belonging to Zap] and sent out an email stating that the January 29, 2014 communications were a mistake." (*Id.* ¶¶ 45–46.) Since then, Zap has struggled to regain its customers' trust and has had to expend time and resources to resecure its computer system and investigate the unauthorized charges and vulnerabilities in its computer system. (*Id.* ¶¶ 47–48, 57–58.) Furthermore, Zap service records indicate that, for the relevant period of time, it was entitled to bill its customers more than $80,000, which it has not recovered. (*Id.* ¶¶ 43–44.)

## II. Procedural History

On November 23, 2015, Zap filed a complaint against Defendants in this Court alleging that Defendants had violated the CFAA, misappropriated trade secrets, and engaged in common law conspiracy and conversion. (*Id.* ¶¶ 49–112.) Defendants filed counterclaims and a complaint against various third parties on January 28, 2016. (Dkt. 17.) On November 16, 2017, the parties participated in a settlement conference, but no settlement was reached. (Dkt. 92.) The parties then engaged in several years of discovery, which was extended numerous times at the request of all parties, and finally concluded on July 3, 2019. (*See generally* Dkts. 19, 39, 46, 48, 50, 58, 68, 75, 78, 80, 94, 104–108, 127.) Plaintiff then moved for summary judgment on Defendants' counterclaims and third-party claims. (*See* Dkt. 137.) The Court granted that motion on September 30, 2020, dismissing Defendants' counterclaims and the third-party Defendants. (*See* Dkt. 140.)

With discovery and motion practice apparently complete, this Court held a conference on May 13, 2021, to set pretrial deadlines and trial dates. (05/13/2021 Docket Order.) At that

conference, however, Defendants informed the Court of their desire to file the present motion for judgment on the pleadings pursuant to Federal Rule of Civil Procedure 12(c) for lack of subject matter jurisdiction. (*See id.*) The motion is now fully briefed. (*See* Defendants' Memorandum of Law in Support of Motion for Judgment on the Pleadings Pursuant to Fed. R. Civ. P. 12(c) ("Def. Mem."), Dkt. 153; Memorandum of Law in Opposition to Defendants' Motion to Dismiss ("Pl. Mem."), Dkt. 154; Defendants' Reply Memorandum of Law in Further Support of Motion for Judgment on the Pleadings Pursuant to Fed. R. Civ. P. 12(c) ("Def. Reply"), Dkt. 155.) For the reasons explained below, the motion is denied in its entirety.

**STANDARD OF REVIEW**

"The standard for granting a Rule 12(c) motion for judgment on the pleadings is identical to that for granting a Rule 12(b)(6) motion for failure to state a claim." *Lively v. WAFRA Inv. Advisory Grp., Inc.*, 6 F.4th 293, 301 (2d Cir. 2021) (quoting *Lynch v. City of New York*, 952 F.3d 67, 75 (2d Cir. 2020)).[2] "To survive such a motion, 'a complaint must contain sufficient factual

[2] It is unclear why Defendants moved under Rule 12(c) rather than Rule 12(b). Rule 12(c) is "little more than a relic of the common law and code eras" and, in contemporary practice, is redundant of Rule 12(b). *Lively*, 6 F.4th at 302. In addition, Defendants' invocation of Rule 12(c) in this case conflates distinct issues. All of the binding precedent on Rule 12(c) liken it to Rule 12(b)(6). *See, e.g.*, *id.* Defendants' only argument that can be characterized as a Rule 12(b)(6) motion, however, is their argument about Plaintiff's CFAA claims. Defendants' arguments that this Court lacks subject matter jurisdiction over M. Weintraub, Dresdner, Weinstock, and Mazal, and should decline to exercise supplemental jurisdiction over Plaintiff's state law claims, are strictly about subject matter jurisdiction and thus properly brought under Rule 12(b)(1), which Defendants never once mention in their papers. *See Brownback v. King*, 141 S. Ct. 740, 749 n.8 (2021) (where "the court might lack subject-matter jurisdiction for non-merits reasons, . . . it must dismiss the case under just Rule 12(b)(1)"). Even Defendants' argument about Plaintiff's CFAA claim, which asserts that Plaintiff fails to plead an element of the only federal claim that would establish federal question jurisdiction, can be addressed under Rule 12(b)(6) *or* Rule 12(b)(1). *Id.*

"In most circumstances, it makes little practical difference whether the district court labels its dismissal of an action as one for lack of subject matter jurisdiction under Rule 12(b)(1) or for failure to state a claim under Rule 12(b)(6)." *Cohen v. Postal Holdings, LLC*, 873 F.3d 394, 399 (2d Cir. 2017) (ellipsis omitted). The two distinctions are: (1) Rule 12(b)(1) dismissals do not have *res judicata* effect; and (2) a court may retain supplemental jurisdiction over state law claims

matter, accepted as true, to "state a claim to relief that is plausible on its face."'" *Vengalattore v. Cornell Univ.*, 36 F.4th 87, 102 (2d Cir. 2022) (quoting *Lynch*, 952 F.3d at 74 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009))). A claim is plausible on its face "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (quoting *Iqbal*, 556 U.S. at 678). The plausibility standard under Rule 12(b)(6) requires "more than a sheer possibility that a defendant has acted unlawfully," and determining whether a complaint meets this standard is "a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Id.* (quoting *Iqbal*, 556 U.S. at 678–79). For purposes of this analysis, the Court "accept[s] as true all factual allegations and draw[s] from them all reasonable inferences; but [it is] not required to credit conclusory allegations or legal conclusions couched as factual allegations." *Hamilton v. Westchester Cnty.*, 3 F.4th 86, 90–91 (2d Cir. 2021) (quoting *Dane v. UnitedHealthcare Ins. Co.*, 974 F.3d 183, 188 (2d Cir. 2020)).

**DISCUSSION**

Until now, this case has proceeded based on the seeming assumption that Plaintiff had plausibly alleged claims against A. Weintraub under the CFAA, giving this Court federal question jurisdiction as to those claims under 28 U.S.C. § 1331 and authority to exercise supplemental jurisdiction over Plaintiff's state law claims against all Defendants under 28 U.S.C. § 1357(a).

---

under 28 U.S.C. § 1367(c) if the dismissal of the federal claims is under Rule 12(b)(6), but not if the dismissal is under Rule 12(b)(1). *Nowak v. Ironworkers Loc. 6 Pension Fund*, 81 F.3d 1182, 1188 (2d Cir. 1996). Here, however, the Court does not dismiss any federal claims, so the distinction is immaterial. Furthermore, even though there would be no *res judicata* effect if the Court dismissed the federal claims under Rule 12(b)(1), the Court would exercise its discretion to retain supplemental jurisdiction over Plaintiff's state law claims given the substantial resources the parties have already spent litigating before this Court. Accordingly, the Court analyzes the motion under the Rule 12(c)/12(b)(6) framework discussed by the parties.

Now, after years of litigation and at the moment trial was to be scheduled, Defendants argue for the first time that the Court lacks jurisdiction over M. Weintraub, Dresdner, Weinstock, and Mazal because no federal claims are alleged against them, that the CFAA claims against A. Weintraub fail as a matter of law, and that the Court should decline to exercise supplemental jurisdiction over Plaintiff's state law claims. The Court entirely disagrees.

## I. Plaintiff's Claims Against Defendants M. Weintraub, Dresdner, Weinstock, and Mazal

Defendants argue that the Court does not have subject matter jurisdiction over Plaintiff's claims against Defendants M. Weintraub, Dresdner, Weinstock, and Mazal because "[n]one of the claims asserted against [these Defendants] remotely involves any question of federal law." (Def. Mem., Dkt. 153, at 4.) This is the first argument in Defendants' motion and does not even purport to rely on Defendants' assertion that Plaintiff's CFAA claims against A. Weintraub must be dismissed. (*Id.* at 3–5.) Defendants instead argue that, regardless of what happens with the CFAA claims against A. Weintraub, Defendants M. Weintraub, Dresdner, Weinstock, and Mazal must be dismissed because the Complaint asserts only state law claims against those Defendants. (*Id.* at 5.)

This argument is late and frivolous. The operative Complaint was filed on November 23, 2015, and has been litigated for nearly seven years now. (*See* Compl., Dkt. 1.) It has been clear from the start that all of the claims against M. Weintraub, Dresdner, Weinstock, and Mazal are based on state law. For Defendants to step up at this late hour and argue for the first time that these claims must be dismissed, simply because they are state law claims, smacks of gamesmanship and a desire to delay trial. Defendants' initial memorandum in support of its motion did not even attempt to argue that Plaintiff's CFAA claims against A. Weintraub are not related to the state law claims against M. Weintraub, Dresdner, Weinstock, and Mazal. (Def. Mem., Dkt.

153, at 4.) Instead, Defendants merely asserted that a federal court simply can never have subject matter jurisdiction whenever only state law claims are brought against a defendant.[3] That position is, of course, flatly incorrect.

Except in certain circumstances not applicable here, 28 U.S.C. § 1367(a) gives federal courts

> supplemental jurisdiction over all other claims that are so related to claims [of which the district courts have original jurisdiction] that they form part of the same case or controversy under Article III of the United States Constitution. Such supplemental jurisdiction shall include claims that involve the joinder or intervention of additional parties.

28 U.S.C. § 1367(a). "A state law claim forms part of the same controversy if it and the federal claim derive from a common nucleus of operative fact . . . *even if the state law claim is asserted against a party different from the one named in the federal claim*." *Briarpatch Ltd. v. Phoenix Pictures, Inc.*, 373 F.3d 296, 308 (2d Cir. 2004) (emphasis added) (internal quotation marks and citations omitted); *see also Exxon Mobil Corp. v. Allapattah Servs., Inc.*, 545 U.S. 546, 558 (2005) ("The last sentence of § 1367(a) makes it clear that the grant of supplemental jurisdiction extends to claims involving joinder or intervention of additional parties."); *F5 Cap. v. Pappas*, 856 F.3d 61, 78 (2d Cir. 2017) ("In enacting the supplemental jurisdiction statute, Congress . . . embraced pendent parties jurisdiction in federal question cases." (internal quotation marks and brackets omitted)); *Hogan v. Consol. Rail Corp.*, 961 F.2d 1021, 1027 (2d Cir. 1992) ("[A] district court generally has supplemental jurisdiction over state-law claims against a non-diverse party if it has original jurisdiction over related claims against another party.").

[3] Defendants acknowledge the existence of diversity jurisdiction under 28 U.S.C. § 1332, which no one has ever attempted to assert in this case, and then waste time vanquishing that strawman of their own creation. (Def. Mem., Dkt. 153, at 4.)

Here, Plaintiff's state law claims against M. Weintraub, Dresdner, Weinstock, and Mazal all "derive from a common nucleus of operative fact" with the federal claims. *Briarpatch*, 373 F.3d at 308. All of the state and federal claims stem from Defendants' alleged scheme to defraud Plaintiff's customers by continuing to bill Plaintiff's customers after Plaintiff's contract with Mazal had expired and by depositing the proceeds of those unauthorized and fraudulent billings in a Mazal bank account. (*See* Compl., Dkt. 1, ¶¶ 24–38, 49–112.)

As noted, Defendants' opening brief in support of its motion did not even attempt to argue otherwise. (Def. Mem., Dkt. 153, at 3–5.) It was only after Plaintiff responded that "the allegations in the Complaint plainly allege a common nucleus of operative fact" (Pl. Mem., Dkt. 154, at 3–5), that Defendants, on reply, attempted to argue that the claims are not part of the same nucleus of operative fact. (Def. Reply, Dkt. 155, at 6–7.) By not making this argument until their reply brief, Defendants have forfeited it. *Browe v. CTC Corp.*, 15 F.4th 175, 191 (2d Cir. 2021) ("[I]t is hornbook law that 'arguments may not be made for the first time in a reply brief.'" (brackets omitted) (quoting *Knipe v. Skinner*, 999 F.2d 708, 710–11 (2d Cir. 1993) (collecting cases)). The Court may thus decline to even consider this argument. *Id.* The Court notes, however, that even if the argument had been timely and properly raised, it is meritless.

In their reply brief, Defendants try to distinguish the CFAA claim against A. Weintraub and the claims against the remaining Defendants by asserting that "[t]he CFAA claim is predicated on the allegation that A. Weintraub had accessed the plaintiff's server 'without authorization' and had caused a 'loss' to the plaintiff that is cognizable under the statute," while the other Defendants are only alleged to have "'opened' or 'created' a bank account into which A. Weintraub had deposited the $80,000 which Plaintiff claims he had diverted from Plaintiff's business." (Def. Reply, Dkt. 155, at 6–7.) That is simply an incorrect reading of the Complaint. In reality, the

Complaint alleges that all Defendants "opened the merchant bank account with full knowledge that it would be used as a depository for illicitly gained monies" (Compl. Dkt. 1, ¶ 31), that the Mazal bank account substantially assisted with the scheme to defraud Plaintiff's customers (*id.* ¶ 92), that M. Weintraub, Weinstock, and Dresdner assisted A. Weintraub in "access[ing] the corporate files of [Zap] pilfer[ing] the personal information and credit card information of the customers of Amp Cellular" (*id.* ¶¶ 32, 77, 79, 92), and that all Defendants "exercised unauthorized dominion and control over Plaintiff['s] funds by stealing and refusing to return the monies" (*id.* ¶ 97).

Defendants' attempt to take a scalpel to the Complaint and excise the allegations about the state-law-claim Defendants' knowing participation in the fraud scheme with A. Weintraub—aside from being carelessly or purposely misleading—is inconsistent with the Court's duty in evaluating a Rule 12(c) or Rule 12(b)(6) motion. *Vengalattore*, 36 F.4th at 102 (quoting *Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842, 854 (2d Cir. 2021) (explaining that, on a Rule 12(c) or 12(b)(6) motion, "[t]he proper question is whether there is a permissible relevant inference from 'all of the facts alleged, taken collectively,' not whether an inference is permissible based on 'any individual allegation, scrutinized in isolation.'") (quoting *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 323 (2007))). Furthermore, Defendants' argument is plainly unavailing. The Complaint clearly ties the creation of the merchant bank account to the actions of A. Weintraub that are alleged to constitute a CFAA violation, and implicates the other Defendants in more of A. Weintraub's actions alleged to violate the CFAA than just opening the bank account. Taken together, the allegations in the Complaint describe a scheme involving all Defendants that gave rise to all counts in the Complaint. Accordingly, even if Defendants' argument attempting to sever

the actions of A. Weintraub from the other Defendants were properly before the Court, it would be rejected.

For all of the reasons explained above, the Court denies Defendants' motion to dismiss the claims against Defendants M. Weintraub, Dresdner, Weinstock, and Mazal. Those claims will proceed to trial.

## II. Plaintiff's CFAA Claims Against Defendant A. Weintraub

Plaintiff asserts two CFAA claims against Defendant A. Weintraub: (1) a claim under 18 U.S.C. § 1030(a)(2)(C), which imposes liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer"; and (2) a claim under 18 U.S.C. § 1030(a)(5)(C), which imposes liability on anyone who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss." 18 U.S.C. § 1030(a)(2)(C), (a)(5)(C); (Compl., Dkt. 1, ¶¶ 49–70).

Defendants argue that (1) under the Supreme Court's recent interpretation of "without authorization" and "exceeded authorized access" in *Van Buren v. United States*, 141 S. Ct. 1648 (2021), the Complaint does not allege that A. Weintraub violated the CFAA, and (2) the Complaint does not allege that Plaintiff suffered a "loss" under the CFAA that would enable Plaintiff to sue. (Def. Mem., Dkt. 153, at 5, 11.)

### A. Without Authorization and Exceeding Authorized Access

The CFAA does not define "without authorization," but does define "exceeds authorized access." Exceeding authorized access means "access[ing] a computer with authorization and to use such access to obtain . . . information in the computer that the accesser is not entitled so to obtain." 18 U.S.C. § 1030(e)(6); *United States v. Valle*, 807 F.3d 508, 523 (2d Cir. 2015). In *Van Buren*, a police sergeant in Georgia named Nathan Van Buren accepted a bribe from an FBI

informant named Andrew Albo to search a state law enforcement database, to which he had authorized access, for a license plate purportedly belonging to a woman who Albo had met at a strip club. 141 S. Ct. at 1652–53. The federal government then charged and successfully prosecuted Van Buren for violating the "exceeds authorized access" clause of 18 U.S.C. § 1030(a)(2). *Id.* at 1653. On appeal, the government's position was that "exceeds authorized access" encompassed misusing access that one otherwise has, while Van Buren argued that "exceeds authorized access" applied only to accessing information to which one's valid access does not extend. *Id.* The Supreme Court sided with Van Buren, finding that because he was authorized to access the information he obtained from the law enforcement computer database, even if he did so for an unauthorized purpose, he did not violate Section 1030(a)(2). *Id.* at 1655.

Importantly, the Court also noted that "[t]he interplay between the 'without authorization' and 'exceeds authorized access' clauses of subsection (a)(2) is particularly probative." *Id.* at 1658.

> The "without authorization" clause . . . protects computers themselves by targeting so-called outside hackers—those who acces[s] a computer without any permission at all. . . . [T]he "exceeds authorized access" clause . . . provide[s] complementary protection for certain information within computers. It does so . . . by targeting so-called inside hackers—those who access a computer with permission, but then "exceed" the parameters of authorized access by entering an area of the computer to which that authorization does not extend.

*Id.* (internal quotation marks, citations, and brackets omitted).

Finally, the Court noted in *Van Buren*—explicitly as dicta that was not necessary to its holding and merely as "extra icing on a cake already frosted"—that "the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity." *Id.* at 1661. The Court observed that "[i]f the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals," such as "an employee who sends a personal email or reads the news using her work computer." *Id.*

As significant as the Supreme Court's holding in *Van Buren* was, it does not "render[] [P]laintiff's CFAA claims against A. Weintraub untenable as a matter of law," as Defendants argue. (Def. Mem., Dkt. 153, at 10.) *Van Buren* is easily and materially distinguishable. In *Van Buren*, the criminal defendant was a police sergeant authorized to use the law enforcement database that he had accessed. 141 S. Ct. at 1654–66. Here, the Complaint alleges that Defendant A. Weintraub accessed Plaintiff's computers and servers *after* he was no longer authorized to do so, having been terminated as Zap's CEO, and Mazal's vendor contract with Zap having expired. (Compl., Dkt. 1, ¶¶ 53–54; *see id.* ¶¶ 25–28, 33–42, 56, 66–68, 73, 78, 84, 90.)

While the Complaint does not explicitly state that A. Weintraub's authorization to access Plaintiff's computers and servers was terminated along with his position as CEO, that is the clear, reasonable inference from the allegations in the Complaint as a whole, which states that A. Weintraub had authorization to access Plaintiff's "accounts, passwords, and other administrative information" solely because of his position as CEO and, after he was terminated as CEO, he accessed Plaintiff's computers and servers "without authorization." (*Id.* ¶¶ 20, 56, 66–68, 73, 78, 84, 90); *Vengalattore*, 36 F.4th at 102 (on a Rule 12(c) or 12(b)(6) motion, courts must draw all permissible relevant inference from all of the facts alleged, taken collectively).

The Court disagrees with Defendants' hyperbolic assertion that A. Weintraub "cannot by any stretch be deemed an 'outside hacker'." (Def. Mem., Dkt. 153, at 10.) Indeed, the reasonable inference to be drawn from Plaintiff's allegations is that after A. Weintraub was terminated as Zap's CEO and after Mazal's contract with Zap had expired, A. Weintraub's alleged accessing of Zap's computer system, for the purpose of committing fraud, amounted to hacking, even if he did not use any advanced or specialized computer skills, as "hackers" sometimes do, to accomplish it. The Court therefore finds, based on the allegations in the Complaint, that A. Weintraub qualifies

as a "so-called outside hacker[] . . . who access[es] a computer without any permission at all[,]" *Van Buren*, 141 S. Ct. at 1658, as to whom Section 1030(a)(2) still applies after *Van Buren*. Furthermore, holding such a former CEO liable for the misconduct alleged here does not run afoul of the Supreme Court's concerns in *Van Buren* about "attach[ing] criminal penalties to a breathtaking amount of commonplace computer activity," "criminaliz[ing] every violation of a computer-use policy," and turning "millions of otherwise law-abiding citizens [into] criminals," such as "an employee who sends a personal email or reads the news using her work computer." *Id.* at 1661. A. Weintraub's alleged conduct was far from "commonplace computer activity," it was already unlawful under state law, as the other claims against him demonstrate, and A. Weintraub was not an employee sending a personal email or reading the news—he was no longer an employee at all, yet was allegedly accessing Zap's computers and servers without authorization to steal confidential client and billing information, and ultimately money.

Defendants contend that because the Complaint alleges that A. Weintraub, while CEO, "had access to [Plaintiff's] accounts, passwords, and other administrative information," "[t]here is thus no question that A. Weintraub was authorized to access the information at issue." (Def. Mem., Dkt. 153, at 8.) This argument completely ignores the allegations in the Complaint and is plainly meritless. Clearly, a CEO or any employee can have authorization to access the company's computers and servers while working there, but lose that authorization upon being terminated from the company—which is what Plaintiff is alleging here as to A. Weintraub. Indeed, as discussed below, courts have accepted this theory of liability and have found terminated employees liable under the CFAA for accessing computers that they were previously authorized to access.

Defendants also argue that, even after A. Weintraub was terminated as CEO, he still "had full access to the company's documents and databases" because he "continued to be a shareholder

of the company." (*Id.* at 8–9.) This argument is completely inappropriate for the present motion, as to which the Court must accept as true all allegations in the Complaint and draw all reasonable inferences in Plaintiff's favor. *Vengalattore*, 36 F.4th at 102. As discussed, the Complaint clearly alleges that Plaintiff revoked A. Weintraub's authorization to access Plaintiff's computers and servers after he was terminated as CEO and once Mazal's vendor contract with Plaintiff ended. The Complaint does not allege that merely being a shareholder authorizes A. Weintraub to access Plaintiff's computers and servers—a proposition that, on its face, seems highly unlikely. Indeed, despite Defendants suggesting that it is an undisputed fact (Def. Mem., Dkt. 153, at 10), Plaintiff's do in fact dispute this assertion, and cite a relevant New York Business Law to the contrary (Pl. Mem., Dkt. 154, at 7 (citing N.Y. Bus. L. § 624).) Defendants offer no evidence to support their contrary position, and even if they did, proffering such evidence to contradict the allegations in the Complaint would be inappropriate on this motion for judgment on the pleadings.[4]

Defendants also inexplicably assert that "[i]t is conceded that this authorization was not revoked or rescinded, explicitly or otherwise." (Def. Mem., Dkt. 153, at 10.) Because of Defendants' passive sentence construction, it is impossible to tell who they believe conceded this fact, but it is surely not Plaintiff. As discussed in detail, Plaintiff's Complaint clearly alleges that A. Weintraub's authorization was revoked after he was terminated as CEO, and Plaintiff explicitly argues that point in opposition to the present motion. (Pl. Mem., Dkt. 154, at 7.)

[4] As discussed, Defendants inexplicably have chosen to make a Rule 12(c) motion after seven years of litigation, and not a summary judgment motion. Indeed, given the history of this case, and Defendants' decision to file what is essentially a Rule 12(b) motion at this late stage in the proceedings, the Court would view any request by Defendants to file for summary judgment with great skepticism.

Defendants next argue that *Advanced Aerofoil Technologies v. Todaro*, No. 11-CV-9505 (ALC) (DCF), 2013 WL 410873 (S.D.N.Y. Jan. 30, 2013), is directly on point. (Def. Mem., Dkt. 153, at 9.) Defendants characterize that case as follows:

> In that case, plaintiff AAT brought a CFAA claim against several former employees who allegedly continued to access AAT's computer system to obtain its confidential information after they had resigned. Noting that AAT had not revoked the former employees' authority to access its computer system at the time of their access of the system, the Court granted defendant's motion to dismiss holding that "plaintiffs cannot state a cognizable claim under CFAA . . . ."

(*Id.* (citation omitted).)

Defendants' description of *Advanced Aerofoil* is misleading, at best. In fact, the complaint in *Advanced Aerofoil* alleged that the defendants had *secretly* resigned and thus the plaintiff "did not know about the resignations and had not terminated [the defendants'] access to its systems." 2013 WL 410873, at *5. Accordingly, in *Advanced Aerofoil*, the court could not reasonably infer from the complaint that the plaintiff had revoked the defendants' authorization to access the relevant information. Here, on the other hand, that is the only reasonable inference to draw from the allegations in the Complaint—which Defendants studiously seek to ignore. Indeed, in *Advanced Aerofoil*, the plaintiff did not even argue that the defendants did not have authorization to access the information at issue, but that the plaintiff "clearly would not have allowed [the defendants] to retrieve its confidential information for the purposes for which [the defendants] ultimately used it." *Id.* That is effectively the same argument ultimately rejected in *Van Buren*, *i.e.*, accessing information that the defendant is authorized to access, but for an unauthorized or improper purpose, does not constitute exceeding authorized access under Section 1030(a)(2). In this case, however, Plaintiff argues that, after being terminated, A. Weintraub was not authorized to access Plaintiff's computers or servers *at all* and that merely by accessing Plaintiff's computer system, Defendant A. Weintraub violated Section 1030(a)(2). (Pl. Mem., Dkt. 154, at 7.)

Furthermore, in *Advanced Aerofoil*, the court explicitly relied on the defendants' status as *current* employees in "declin[ing] the opportunity to expand the CFAA to include situations where *an employee* takes confidential information, using authorization given to him and controlled by his employer." *Id.* at *7 (emphasis added). Here, the Court similarly is not expanding the CFAA to include situations where an employee took confidential information by using authorization given to him by his employer, but is applying the CFAA to a situation where an *ex*-employee allegedly took confidential information by using authorization that had been *revoked* by his employer.[5]

Finally, Defendants argue that,

> [w]hile the Second Circuit has not specifically addressed the question whether an ex-employee whose access to his former employer's computer has not been revoked can be deemed to act "without authorization" in accessing it, the Ninth Circuit has answered this question firmly in the negative. If the computer owner has not affirmatively rescinded the defendant's right to access the computer, any existing authorization/permission remains. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134–35 (9th Cir. 2009).

(Def. Mem., Dkt. 153, at 10.) This argument rests on both a mischaracterization of the Complaint and a mischaracterization of *LVRC*. First, Plaintiff's argument once more assumes that the Complaint alleges that A. Weintraub's authorization to access Plaintiff's computers and servers had "not been revoked" when he was terminated. The Court will not belabor this point, but as discussed, the only reasonable inference to draw from the Complaint as a whole is that A. Weintraub's authorization had been revoked by the time he began accessing Zap's computers as part of the alleged fraud scheme. Plaintiff's opposition to the present motion confirms that reading.

[5] *Loop AI Labs. Inc. v. Gatti*, No. 15-CV-798 (HSG), 2015 WL 5158639, at *3 (N.D. Cal. Sept. 2, 2015), also cited by Defendants (Def. Mem., Dkt. 53, at 9), similarly involved a plaintiff arguing that a defendant's authorization had been "impliedly revoked" when the defendant began working for another company but was still employed by the plaintiff. *Id.* That case actually strongly supports Plaintiff's position, noting that if any of the alleged access had occurred after the defendant had actually stopped working for plaintiff, that would have constituted a CFAA violation. *Id.*

(Def. Mem., Dkt. 154, at 7.) Second, Defendants' citation to *LVRC* for the above proposition, like Defendants' characterization of *Advanced Aerofoil*, is grossly misleading. *LVRC* says absolutely nothing about an *ex*-employee accessing his former employer's computer.

In *LVRC*, an employee accessed a company computer *while he was an employee*, then emailed the information to himself and his wife, and later viewed that information on his own computer after he was no longer an employee. 581 F.3d at 1129–30. The court's holding, finding no liability under Section 1030(a)(2), was entirely based on the fact that the defendant's "access occurred *during the term of his employment*." *Id.* at 1132–33 (emphasis added). As to emailing the information to himself and accessing it later, the Court noted that the defendant had not accessed the company's computer after his employment, and that "there was no evidence that [the defendant] had agreed to keep the emailed documents confidential or to return or destroy those documents upon the conclusion of his employment." *Id.* at 1132. By contrast, in this case, the information was in fact confidential and was allegedly taken by A. Weintraub only after he had been terminated from Zap. Here, there are no allegations, like those in *LVRC*, that A. Weintraub accessed the confidential information while serving as Zap's CEO, emailed it to himself, and then later accessed it on his own computer. Indeed, much of the relevant information, such as customer charges for subsequent months, was necessarily generated after A. Weintraub was terminated as CEO in September 2013. Accordingly, *LVRC* does not support Defendants' position.[6]

Lastly, the Court must note that Defendants argue that *Van Buren*'s construction of the CFAA was the law in this Circuit since 2015, when the Second Circuit decided *Valle*, 807 F.3d at

[6] Defendants also cite *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016), for the proposition that the "without authorization" provisions of the CFAA are only violated "when [a defendant] has no permission to access a computer or when such permission has been revoked explicitly." (Def. Mem., Dkt. 153, at 10.) Again, in this case, Plaintiff alleges that A. Weintraub's authorization was explicitly revoked. (*See* Pl. Mem., Dkt. 154, at 7.)

523–28, and that this construction was fastidiously followed by the lower courts of this Circuit. (Def. Mem., Dkt. 153, at 6–8.) Defendants are actually correct on this point. However, that does not help them because, as discussed, *Van Buren*'s construction of the CFAA does not support their position nor bar Plaintiff's CFAA claims against A. Weintraub. Indeed, it has been consistently noted by courts in this Circuit that allegations that an ex-employee accessed their former employer's computers or servers after that access had been revoked would state a claim under the CFAA.[7] *Sell It Soc., LLC v. Strauss*, No. 15-CV-970 (PKC), 2018 WL 2357261, at *3 (S.D.N.Y. Mar. 8, 2018) (collecting cases); *Apple Mortgage Corp. v. Barenblatt*, 162 F. Supp. 3d 270, 287 (S.D.N.Y. 2016); *Amphenol Corp. v. Paul*, 993 F. Supp. 2d 100, 110 (D. Conn. 2014); *Poller v. BioScrip, Inc.*, 974 F. Supp. 2d 204, 233 (S.D.N.Y. 2013); *Advanced Aerofoil*, 2013 WL 410873, at *5.[8]

[7] The fact that the Supreme Court's holding in *Van Buren* has been the law in this Circuit since 2015—the year this lawsuit was filed—again raises the question of why Defendants waited until 2021, almost on the eve of trial, to raise this argument as a basis for dismissal under Rule 12(c). Defendants' current counsel appeared in this case on May 9, 2018, a full three years before raising the issues in this motion. (See Dkts. 98, 99.) And while Defendants' brief relies extensively on *Van Buren*, that case was decided after the pre-motion conference on Defendants proposed Rule 12(c) motion and thus could not have been the impetus for Defendants late-filed Rule 12(c). The Court again voices its concerns about Defendants' motivation and the specter of bad faith and dilatory tactics in order to cause undue delay and prejudice to Plaintiff. The defense is on notice that the Court will not permit the defense to engage in such tactics to delay trial in this case and that the Court has given serious consideration to whether sanctions are appropriate, given how defense counsel has handled this case, including all of the last-minute, meritless arguments and mischaracterization of cases that Defendants have made in the present motion.

[8] To the extent Defendants are arguing that A. Weintraub was still "authorized" to access Plaintiff's computers and servers because he somehow was still able to log into those computers and servers, that argument is also incorrect. *Sell It Soc.*, 2018 WL 2357261, at *3 ("Persuasive precedent and common sense . . . belie [the defendant's] argument, which equates having login credentials with being authorized to access the database." (collecting cases)); *Poller*, 974 F. Supp. 2d at 233 ("[W]here an employee has certain access to a computer or system associated with her job, that access will be construed as unauthorized within the meaning of the CFAA only where it occurs after the employee is terminated or resigns."); *see Apple Mortgage Corp.*, 162 F. Supp. 3d at 287; *Amphenol Corp.*, 993 F. Supp. 2d at 110.

For all of the reasons explained above, Defendant's "without authorization" argument fails, and Plaintiff's CFAA claims against A. Weintraub will proceed to trial.

**B. Plaintiff's Private Right of Action under the CFAA**

The CFAA is both a criminal and civil statute. 18 U.S.C. § 1030(a)(2)(B); *Valle*, 807 F.3d at 523. "A civil action for a violation of [the CFAA] may be brought [by a private person or entity] only if the conduct involves":

> (I) loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value; (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; [or] (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security.

18 U.S.C. § 1030(g), (c)(4)(A)(i)(I)–(V). The only subsection at issue here is "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." *Id.* § 1030(c)(4)(A)(i)(I).

The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11). In addition, "[d]amages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages." *Id.* § 1030(g); *Hancock v. Cnty. of Rensselaer*, 882 F.3d 58, 64 (2d Cir. 2018).

Plaintiff has adequately alleged more than $5,000 of economic damages that occurred during a one-year period and stemmed from both "revenue lost . . . because of interruption of service" and the cost of "responding to an offense [and] conducting a damage assessment." 18 U.S.C. § 1030(e)(11). Plaintiff lost roughly $80,000 of revenue within six months as a direct result

of A. Weintraub's alleged unauthorized computer access and Defendants' fraud scheme. (Compl., Dkt. 1, ¶¶ 43–44.) Common sense and a reasonable inference from the Complaint also demonstrate that Plaintiff expended economic resources to "investigate the unauthorized charges, investigate vulnerabilities in the security of the computer system, and re-secure the computer system." (*Id.* ¶ 69.)

Nevertheless, Defendants attempt to argue that Plaintiff has not alleged a loss cognizable under the CFAA. Once again, like all of Defendants' arguments in the present motion, this argument is based on a blatant misreading of the case law and is brought inappropriately late in the litigation. First of all, Defendants conflate "revenue lost . . . because of interruption of service" and the cost of "responding to an offense [and] conducting a damage assessment." They rely on a number of district court cases which, under Defendants' reading, held that only losses "related to remedying any damage to plaintiff's computer" are cognizable under the CFAA. (Def. Mem., Dkt. 153, at 12–13.) Those cases, however, all discuss the types of losses cognizable for investigations related to unauthorized computer access, not lost revenue. "[T]he plain language of [§ 1030] treats lost revenue as a different concept from incurred costs." *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 562 (2d Cir. 2006). Here, Plaintiff clearly alleges that it lost revenue because of the interruption of its billing service caused by Defendants' conduct, and Defendants simply have no valid argument that such a loss is not cognizable under the CFAA. Indeed, it would be absurd to conclude that revenue diverted from a plaintiff's billing service by someone hacking into the plaintiff's computers and servers would not be cognizable under the CFAA.

Furthermore, Defendants read the district court cases about losses associated with investigations far too narrowly. It is true that courts in this district are "reluctant to allow losses stemming from prophylactic preventative measures to constitute 'losses' under the statute, even if

such measure is prompted by a specific breach." *Reis, Inc. v. Spring11 LLC*, No. 15-CV-2836 (PGG), 2016 WL 5390896, at *8 (S.D.N.Y. Sept. 26, 2016) (brackets omitted). However, "[t]he weight of caselaw in this Circuit holds that a Plaintiff can satisfy the CFAA § 1030(g) 'damage or loss' requirement by pleading a loss stemming from a damage assessment and/or remedial measures, even without pleading actual damage." *Id.* (collecting cases) (brackets omitted). "For example, if the alleged loss seeks to identify evidence of a breach of computer security, assess any damage it may have caused, and determine whether any remedial measures were needed to resecure the network, then it qualifies as a 'loss' pursuant to the CFAA." *Id.* (collecting cases) (internal quotation marks and brackets omitted). In addition, the Second Circuit has recently held that the cost of "investigat[ing] . . . unauthorized access to [a database]" qualifies as a "cost[] of 'conducting a damage assessment'" under the CFAA. *Saunders Ventures, Inc. v. Salem*, 797 F. App'x 568, 570, 572 (2d Cir. 2019). These are the exact types of allegations Plaintiff puts forth here. (Compl., Dkt. 1, ¶ 69 (alleging that the breach prompted Plaintiff to "investigate the unauthorized charges, investigate vulnerabilities in the security of the computer system, and re-secure the computer system").)

Finally, the Court must note once again that the argument that Plaintiff did not plead a loss cognizable under the CFAA could have been made at any stage of the litigation, but Defendants waited to raise it until virtually the eve of trial. That is entirely inappropriate. Discovery has closed. If, at this stage, Defendants believe that Plaintiff has no evidence that Plaintiff actually suffered a loss cognizable under the CFAA, Defendants should have moved for summary judgment. The fact that they did not do so only reinforces how meritless this argument is.

## III. Supplemental Jurisdiction

Even if this Court were to dismiss Plaintiff's CFAA claims, it would retain jurisdiction over Plaintiff's state law claims. As discussed, the Court has supplemental jurisdiction over the

state law claims in this case pursuant to 28 U.S.C. § 1367(a). "In order for a district court to decline to exercise supplemental jurisdiction, where section 1367(a) is satisfied, the discretion to decline supplemental jurisdiction is available *only if* founded upon an enumerated category of subsection 1367(c)." *Catzin v. Thank You & Good Luck Corp.*, 899 F.3d 77, 85 (2d Cir. 2018). One of those subsections is where "the district court has dismissed all claims over which it has original jurisdiction." *Id.* (quoting 28 U.S.C. § 1367(c)(3)). "[I]n the usual case in which all federal-law claims are eliminated before trial, the balance of factors to be considered under the pendent jurisdiction doctrine—judicial economy, convenience, fairness, and comity—will point toward declining to exercise jurisdiction over the remaining state-law claims." *Valencia ex rel. Franco v. Lee*, 316 F.3d 299, 305 (2d Cir. 2003).

However, even "[w]hen § 1367(c)(3) applies, the district court must still meaningfully balance the supplemental jurisdiction factors" and, ultimately, "[t]he declining of supplemental jurisdiction must actually promote those values." *Catzin*, 899 F.3d at 81–82, 85–86 (reversing the district court's decision to decline supplemental jurisdiction when federal claims were dismissed on "the eve of trial" based on speculation that the plaintiffs brought their federal claims just to be in federal court).

Here, even if the Court were to dismiss all of Plaintiff's federal claims, the declining of supplemental jurisdiction would not "actually promote" judicial economy, convenience, fairness, or comity. To the contrary, declining supplemental jurisdiction after extensive discovery and motion practice has taken place in this Court—and sending this case to a new court unfamiliar with its details and history—would actively work against the values of judicial economy, convenience, and fairness. Such a result would be particularly and acutely unfair here, given, as repeatedly noted, Defendants' decision to wait until almost the eve of trial to make a motion that

could and should have been made at the beginning of this case, some seven years ago. Finally, this case involves relatively common, run-of-the mill state law claims, so comity would not be offended by this Court retaining supplemental jurisdiction even if only state law claims remained.

**CONCLUSION**

For all of the reasons explained above, Defendants' motion for judgment on the pleadings is denied in its entirety. The parties shall submit a new joint pretrial order on or before October 20, 2022, and the Court will set a date for an Initial Pretrial Conference at which a trial date and related deadlines will be set.[9]

SO ORDERED.

*/s/ Pamela K. Chen*
Pamela K. Chen
United States District Judge

Dated: September 19, 2022
Brooklyn, New York

[9] As the Court has noted at various points in this decision, because Defendants chose to wait until now to file a Rule 12(b)(6) motion—a motion that could and should have been filed at the outset of litigation—the Court will look askance at any request by Defendants to file a summary judgment motion. As discussed, had discovery in this case over the past seven years yielded evidence to support such a motion, *that* is the motion that Defendants should have filed before trial, instead of the one they chose to file. Indeed, Defendants only requested permission to file the instant motion *after* discovery had long closed, *after* the parties had filed a Joint Pretrial Order in preparation for trial, and *at* the Initial Pretrial Conference held by the Court to *prepare for trial*. As it is, the Court finds that the current motion is entirely frivolous and borderline sanctionable. The Court will not allow Defendants to further waste Plaintiff's or the Court's time and resources with a frivolous summary judgment motion. Thus, the parties should prepare to move forward to trial.